

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*

395 Shakespeare Drive, Morrisville, NC

Case No.

1:20mj330

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 1030(a)(2)	Computer fraud
18 U.S.C. § 1956; § 1028A	Laundering of monetary instruments; aggravated identity theft

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of days *(give exact ending date if more than 30 days)*: is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ KIRK ELLIS

Applicant's signature

Kirk Ellis, Special Agent

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date:

11/2/2020

City and state: Winston-Salem, North Carolina

Joi Elizabeth Peake
Judge's signature

Hon. Joi Elizabeth Peake, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Kirk Ellis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant. The application relates to an investigation of Charisma Fozard and Marcus Thomas, a married couple. Based on my investigation, I believe that Fozard and Thomas currently reside at 395 Shakespeare Drive, Morrisville, NC, hereinafter "Premises." Fozard is an attorney licensed in North Carolina and South Carolina. The website of the North Carolina Secretary of State lists the Premises as the location of the Law Office of Charisma Fozard PLLC. Investigators intend to use the attached filter procedures to minimize the review and retention of privileged materials.

2. Database searches reveal that Charisma Fozard is listed as the joint/secondary owner of a 2014 red Mazda 6 with North Carolina Plate TBB2482, hereinafter "Mazda 6"; Charisma Fozard's father, Donald Fozard is listed as the primary owner. Database searches reveal that Marcus Thomas is listed as the owner of a 2015 white GMC Yukon Denali with North Carolina Plate FKR7380, hereinafter "GMC Yukon Denali." On February 7, 2020, and on October 22, 2020, the Mazda 6 was parked on a public street in front of the Premises, and the GMC Yukon Denali was parked in the driveway of the Premises.

3. I am a Special Agent with the Defense Criminal Investigative Service (DCIS), and have been employed in the DCIS Cyber-Crimes section since July 2018. Prior to my current

assignment, I was a ten-year veteran Special Agent with the United States Army Criminal Investigation Division conducting a variety of investigations including financial and computer crimes investigations, and performing digital forensics. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am authorized by law to conduct investigations and make arrests for felony offenses. The Cyber-Crimes section investigates, among other things, crimes involving the unauthorized intrusion into computers and computer systems, which is one of the offenses at issue here. Based upon my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various criminal offenses. I am also a certified computer forensics agent, trained in aspects of recovering electronic evidence in a format presentable as evidence in court. As part of my duties, I investigate criminal violations relating to 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1030(a)(2) (Computer Fraud), 18 U.S.C. § 1956 (Laundering of Monetary Instruments), and 18 U.S.C. § 1028A (Aggravated Identity Theft). I have received training and instruction in the field of investigation of financial and computer crimes and have participated in investigations involving electronic evidence, emails, text messages, and the Internet.

4. Based on the evidence described in this affidavit, there is probable cause to believe that evidence related to violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1030(a)(2) (Computer Fraud), 18 U.S.C. § 1956 (Laundering of Monetary Instruments), and 18 U.S.C. § 1028A (Aggravated Identity Theft) is located at the Premises, in the Mazda 6, in the GMC Yukon Denlia, on the person of Charisma Fozard, and on the person of Marcus Thomas.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

6. On March 8, 2019, I received MyPay records from Special Agent Jaime Jones (Defense Finance and Accounting Service (DFAS), Internal Review, Criminal Investigations Branch (DICIB), Indianapolis, IN) regarding an ongoing investigation involving the fraudulent diversion of funds from the MyPay accounts of five retired military personnel (hereinafter, "VICTIM-01" through "VICTIM-05").

7. MyPay is an online account management system used by active and retired military personnel, as well as Department of Defense civilian employees. MyPay customers can manage most aspects of their pay and financial records by remotely accessing the system with a Username and Password.

- a. The MyPay Master PIN Database resides on a server that is physically located in the Middle District of Pennsylvania. When a user enters logon credentials to access a MyPay account, that information is transmitted from the user location through the Master PIN Database in the Middle District of Pennsylvania.
- b. The MyPay servers that hold user data are physically located in Georgia. When a user views or makes changes to information in a MyPay account, that information is transmitted between the user location and the MyPay servers in Georgia.

8. A review of MyPay network logs revealed that between September 9, 2018, and February 10, 2019, unknown individual(s) fraudulently accessed the MyPay accounts of the VICTIMS from multiple IP addresses. After gaining access to the MyPay accounts, the individual(s) changed the direct deposit accounts from the authorized bank accounts to American Express Bluebird accounts. Based on these changes, each of the VICTIMS suffered a loss of at least one month's retirement payment.

9. American Express Bluebird accounts are online membership-based accounts. Email accounts are required in order to setup a Bluebird account. Members can transfer funds between Bluebird accounts for free, and can send funds to be picked up at any Wal-Mart location. Transfers from a Bluebird account to a Wal-Mart location are facilitated by RIA Financial Services. When an individual retrieves funds at Wal-Mart, they are frequently identified with a form of photo identification, such as driver's license or passport. When a peer-to-peer (P2P) transfer is completed between two Bluebird accounts, an email is typically sent to the email account associated with the receiving Bluebird account.

10. In March, April, June, and July 2019, Grand Jury subpoenas were served on American Express for information pertaining to the fraudulent direct deposit accounts and accounts associated with the original fraudulent direct deposit accounts.

11. In April 2019, a Grand Jury subpoena was served on Oath, Inc. for information pertaining to AOL email accounts associated with the fraudulent bank accounts.

12. In May 2019, two Grand Jury subpoenas were served on Google, Inc. for information pertaining to Gmail accounts that were associated with the fraudulent bank accounts or otherwise associated with the fraud scheme. One of the email accounts subpoenaed was slimshaddy2bk@gmail.com (hereinafter, "ARIAS EMAIL-01"). The phone number associated with that account was listed as (407) 720-4668 (hereinafter, "ARIAS PHONE").

13. On September 11, 2018, American Express Bluebird account *0648 was opened with the account owner listed as Ronald Vitarella, 428 S. Walnut St, Ravenna, OH (hereinafter, "VITARELLA ACCOUNT"). The email address associated with the account is ceperez41@aol.com (hereinafter, "ARIAS EMAIL-02"). The recovery email for ARIAS EMAIL-02 is ARIAS EMAIL-01. Three phone numbers were listed as associated with the account, including ARIAS PHONE. Records indicate over 40 emails were sent to ARIAS EMAIL-02 between September 11, 2018, and January 12, 2019, regarding financial transactions related to the VITARELLA ACCOUNT. On October 26, 2018, the retirement pay for VICTIM-02 in the amount of \$2,017.63 was deposited into the VITARELLA ACCOUNT. On December 26, 2018, the retirement pay for VICTIM-04 in the amount of \$1,811.10 was deposited into the VITARELLA ACCOUNT. These funds were subsequently withdrawn through a series of ATM withdrawals and an electronic funds transfer.

14. On October 28, 2019, Isabel Bailey was interviewed. Bailey is the sister of Vitarella. Bailey stated that Vitarella was currently in the Philippines. She further revealed that she was in contact with the individual who directed Vitarella to open the VITARELLA

ACCOUNT as well as other bank accounts. This individual is known to Bailey as Martha Arias. Bailey came to know Arias in January 2019 after being introduced to Arias by Vitarella. Arias has directed Bailey to open multiple bank accounts, has had money sent to Bailey via numerous methods, and has directed Bailey to send the funds to other individuals via numerous methods. These methods included electronic money transfer services and mailing money orders and cash. Arias also directed Bailey to purchase a printer and check stock to print checks. Additionally, Arias obtained Bailey's personal information from her and opened accounts in Bailey's name. Arias communicates with Bailey via email through email addresses ARIAS EMAIL-01 and ARIAS EMAIL-02, and via text messages from ARIAS PHONE.

15. On September 29, 2018, American Express Bluebird account *3131 was opened with the account owner listed as Joseph Bell, 37 Spring St, Phoenix, NY (hereinafter, "BELL ACCOUNT"). The email address associated with the account is dabluech22@gmail.com (hereinafter, "BELL EMAIL"). Records indicate over 40 emails were sent to BELL EMAIL between September 29, 2018, and March 21, 2019, regarding financial transactions related to the BELL ACCOUNT. On January 28, 2019, the retirement pay for VICTIM-01 in the amount of \$1,973.33 was deposited into this account. On the same day, two P2P transfers totaling \$1,705.00 were sent to a Bluebird account with the associated email address thuonganderson@gmail.com (hereinafter, "WILLIAMS EMAIL-01"), and one P2P transfer for \$268.00 (totaling \$1,973.00) was sent to a Bluebird account with associated email address gailcurby0819@gmail.com (hereinafter, "WILLIAMS EMAIL-02").

- a. On January 7, 2019, American Express Bluebird accounts *7008 and *3007 were opened with the account owner listed as Gladys Williams, 518 N. 4th St, Toronto, OH (hereinafter, "WILLIAMS ACCOUNT-01" and "WILLIAMS ACCOUNT-02"). The email address associated with WILLIAMS ACCOUNT-01 is WILLIAMS EMAIL-01. The email address associated with WILLIAMS ACCOUNT-02 is WILLIAMS EMAIL-02. On January 28, 2019, WILLIAMS ACCOUNT-01 received \$1,705.00 in P2P transfers from the BELL ACCOUNT and WILLIAMS ACCOUNT-02 received \$268.00 in a P2P transfer from the BELL ACCOUNT. Records indicate emails were sent to both WILLIAMS EMAIL-01 and WILLIAMS EMAIL-02 regarding the transactions on January 28, 2019. On January 28 and 29, 2019, the following transfers were sent from the BELL ACCOUNT: two P2P transfers of \$500.00 were sent to a Bluebird account with associated email address jtejeda81691@gmail.com; three P2P transfers of \$500.00, \$238.00, and \$260.00 were sent to a Bluebird account with associated email address debbie90bb@gmail.com; two P2P transfers of \$500.00 and \$356.00 were sent to a Bluebird account with associated email address supermicah1210@gmail.com.
- b. On December 29, 2018, WILLIAMS EMAIL-02 was accessed from 173.234.142.107. Seven hours later, on December 30, 2018, WILLIAMS EMAIL-01 was accessed from the same IP address.

16. On October 28, 2019, Gladys Williams was interviewed. Williams related she met an individual known to her as John Tello through Google Hangouts. Tello portrayed himself as a member of the U.S. military, and established an online relationship with Williams. Through this relationship, he obtained Williams' personal information from her. Tello directed Williams to open bank accounts, and also opened bank accounts in her name. When bank cards arrived at her house, she sent pictures of the bank cards to Tello via messages to his phone number. Williams communicated with Tello via Google Hangouts and text message.

17. On August 13, 2018, American Express Bluebird account *9953 was opened with the account owner listed as Roy Ehlers, 1852 Campbell Ave, Thousand Oaks, CA (hereinafter, "EHLERS ACCOUNT"). The email address associated with the account is royj015@perfectedhomesandcare.com. On January 28, 2019, the retirement pay of VICTIM-05 in the amount of \$2,986.64 was deposited into the EHLERS ACCOUNT. On the same day, \$1,350.00 was sent in a P2P transfer to a Bluebird account with associated email address jetkenny7@gmail.com (hereinafter, "JONES EMAIL"). An additional \$1,100.00 was sent in a P2P transfer to a Bluebird account with associated email address jforman@gmx.com (hereinafter, "ALSTON EMAIL-01").

- a. On November 24, 2018, American Express Bluebird account *2025 was opened with the account owner listed as Tynautica Jones, with a registered address of the Premises (hereinafter, "JONES ACCOUNT"). The email address associated with the account is JONES EMAIL. The JONES ACCOUNT received the

aforementioned \$1,350 in P2P transfers from the EHLERS ACCOUNT on January 28, 2019. Less than 30 minutes later, on the same day, \$2,460.00 was sent from the JONES ACCOUNT to Charisma Fozard via RIA transfer, retrieved at Wal-Mart in Durham, NC. Charisma Fozard's passport was recorded as the identification used at pickup. The Wal-Mart location was approximately 12 miles from the Premises. Previously, on January 23 and 24, 2019, \$1,300.00 and \$1,100.00 were sent from the JONES ACCOUNT to Marcus Thomas via RIA transfer, retrieved at Wal-Mart in Morrisville, NC. Marcus Thomas's North Carolina driver's license was recorded as the identification used at pickup. The Wal-Mart location was approximately 3 miles from the Premises. Between January 22, 2019, and January 29, 2019, over \$4,000.00 was withdrawn from the JONES ACCOUNT at ATMs located in Research Triangle, NC. Research Triangle, NC, is less than 5 miles from the Premises.

- b. On December 3, 2018, American Express Bluebird account *7456 was opened with the account owner listed as Rashanda Alston, with a registered address of the Premises (hereinafter, "ALSTON ACCOUNT-01"). The email address associated with the account is ALSTON EMAIL-01. The ALSTON ACCOUNT-01 received the aforementioned \$1,100.00 in P2P transfers from the EHLERS ACCOUNT on January 28, 2019. On the same day, \$550.00 was transferred from ALSTON ACCOUNT-01 P2P to the JONES ACCOUNT, and \$1,659.10 was transferred

from ALSTON ACCOUNT-01 to a Citibank account. Between January 23, 2019, and January 29, 2019, over \$4,000.00 was withdrawn from the ALSTON ACCOUNT-01 at ATMs located in Research Triangle, NC.

- c. On November 16, 2018, American Express Bluebird account *3521 was opened with the account owner listed as Alston, with a registered address of the Premises (hereinafter, "ALSTON ACCOUNT-02"). The email address associated with the account is rashandamomma@gmail.com (hereinafter, "ALSTON EMAIL-02"). The ALSTON ACCOUNT-02 received numerous transfers from other American Express Bluebird accounts. On December 15, 2018, \$1,260.00 was sent to Marcus Thomas via RIA transfer, retrieved at a Wal-Mart in Morrisville, NC. Marcus Thomas's North Carolina driver's license was recorded as the identification used at pickup. The Wal-Mart location was approximately 3 miles from the Premises. On December 21, 2018, \$1,250.00 was sent to Marcus Thomas via RIA transfer, retrieved at a Wal-Mart in Raleigh, NC. Marcus Thomas's North Carolina driver's license was recorded as the identification used at pickup. The Wal-Mart location was approximately 23 miles from the Premises. Between December 14, 2018, and December 26, 2018, over \$5,000.00 was withdrawn from ALSTON ACCOUNT-02 at ATMs located in Morrisville, NC, and Research Triangle, NC.

18. In July 2019, a Grand Jury subpoena was served on Charter Communications for information pertaining to IP addresses linked to bank accounts and email accounts involved in this

fraud scheme. Multiple IP addresses were found to be associated with the Premises. The Charter Communications account associated with the Premises was registered in the name James Lyons. The following activity is associated with IP addresses associated with the Premises:

- a. On January 17, 2019, the JONES EMAIL was accessed from IP address 2606:a000:46c7:d300:101b:9379:c841:a40f.
- b. Between January 17, 2019, and January 28, 2019, the JONES ACCOUNT was accessed from IP address 45.37.86.97 on numerous occasions.
- c. Between January 18, 2019, and January 28, 2019, the ALSTON ACCOUNT-01 was accessed from IP address 45.37.86.97 on numerous occasions.
- d. ALSTON EMAIL-02 was accessed from IP address 2606:a000:46c7:d300:bc11:b05c:b9b7:9a02 on March 14, 2019.

19. In April 2019, a Grand Jury subpoena was served on RIA Financial Services for information pertaining to RIA transfers associated with individuals identified through the fraudulent accounts. The following activity was noted during the review:

- a. Over \$80,000 was sent from 25 different individuals who had a registered address of the Premises between August 27, 2018, and February 27, 2019.
- b. Marcus Thomas received over \$40,000 in RIA transfers from multiple individuals between August 27, 2018, and February 13, 2019. Each of these individuals had a registered address of the Premises.

- c. Charisma Fozard received over \$13,000 in RIA transfers from multiple individuals between December 26, 2018, and February 27, 2019. Each of these individuals had a registered address of the Premises.

20. In May 2020, a court order was served on Apple, Inc. for records pertaining to marcusathomas@me.com, an account connected to Marcus Thomas through information obtained during this investigation. The records revealed the account was registered to Marcus Thomas and was associated with the Premises. Additionally, the records revealed several Apple devices registered to the account including multiple Apple iPhones.

21. The investigation has also revealed that Marcus Thomas and Charisma Fozard are involved in other financial transactions—similar to those described above—involving cash deposits and withdrawals and the use of money transfer services such as Apple Cash, Square Cash and Western Union. Specifically, between January 2019 and April 2020, Marcus Thomas and Charisma Fozard had at least 10 bank accounts open in their names. The accounts in Marcus Thomas' name (some of which are held jointly with Charisma Fozard) received over \$350,000 in deposits from numerous sources between January 2019 and February 2020. In the same time period, there was over \$170,000 in cash withdrawals from the accounts. There was over \$40,000 in Coinbase (cryptocurrency) transactions. Approximately \$45,000 was paid to other individuals and businesses in transactions \$500 or larger. Several transfers were made between accounts belonging to both Marcus Thomas and Charisma Fozard. There was over \$450,000 in transfers moving money between accounts owned by Marcus Thomas or Charisma Fozard. Between

January 2019 and January 2020, the accounts in only Charisma Fozard's name received approximately \$96,000 in deposits from numerous sources. In the same time period, there was over \$50,000 in cash withdrawals from the accounts. Approximately \$24,000 was paid to other individuals and businesses in transactions \$500 or larger.

22. Database checks revealed the following:

- a. Rashanda Alston is shown to have resided at an address in Louisburg, NC, from approximately October 2016 through April 2019. Alston's North Carolina driver's license lists an address in Creedmoor, NC. There is no known association of Alston with the Premises, other than bank accounts.
- b. Tynautica Jones is shown to have resided at multiple addresses in Henderson, NC, between December 2017 and February 2019. There is no known association of Jones with the Premises, other than bank accounts.

23. Database research conducted on Marcus Thomas revealed two different Social Security Numbers associated with him. This database research suggests both Social Security Numbers have been associated with Marcus Thomas through credit reporting bureaus. Coordination with the Social Security Administration revealed one of these Social Security Numbers was invalid. The states of both Ohio and North Carolina list valid driver's licenses for Marcus Thomas. Both of these driver's licenses were obtained using Marcus Thomas's valid Social Security Number.

24. Based on my training and experience, I know that individuals who commit fraud schemes often maintain books, records, receipts, notes, ledgers, and other documents (in paper and electronic form) relating to the scheme. It is common, moreover, for individuals who commit fraud schemes to maintain these records for extended periods and to maintain these records where they have ready access to them, including their residences, vehicles, in electronic format on computers and mobile devices, and on their person.

25. Based on my training and experience, I know that individuals involved in transnational fraud schemes commonly use numerous methods to facilitate the movement of funds and to conceal the origins of the funds. Some of these methods include the purchase and export of various items including but not limited to information technology equipment and automobiles; the use of money transfer services including but not limited to Western Union, MoneyGram, RIA Financial Services, Paypal, Venmo, Square, CashApp, and Zelle; the use of wire transfers; the use of crypto-currencies; sending and receiving cash via mail services such as USPS, UPS and FedEx; and sending and receiving gift cards (usually by photographs sent via text messages or other mobile messaging applications).

26. The interviews of Bailey and Williams revealed that both text messages and emails are a common means of communication within this fraud scheme. Interviews with other individuals involved in similar transnational fraud schemes have revealed that text messages, messages through phone applications such as WhatsApp and Kik, and email are the most common methods of communication.

27. Based on my training and experience, I know that individuals frequently communicate with others and conduct online banking through electronic devices that they often physically possess on their person.

28. As noted above, Charisma Forzard is believed to be a licensed attorney, and the website of the North Carolina Secretary of State lists the Premises as the location of the Law Office of Charisma Fozard PLLC. The business was registered with the North Carolina Secretary of State on October 1, 2019. Articles of Organization obtained from the North Carolina Secretary of State list the business address as 2530 Meridian Parkway, Unit 2011, Durham, NC. When a web search for "Law Office of Charisma Fozard" was conducted, only two results were returned. These results contained basic information similar to what was found on the North Carolina Secretary of State website. No website was found for the Law Office of Charisma Fozard.

29. Surveillance has been conducted on the Premises on multiple occasions in February, March, and October 2020. There is no outward appearance of a law office operating in the Premises. No signage has been observed indicating or advertising the Premises as a law office. No foot-traffic has been observed in or out of the residence. The only vehicles observed at the residence have been the Mazda 6 and GMC Yukon Denali as well as a late-model black Chevrolet Suburban with North Carolina plate ID-154214. The dealer plate on the black Chevrolet Suburban is registered to Arrow Motors, LLC. Arrow Motors, LLC, is a dissolved North Carolina business of which Marcus Thomas was listed as a member. Arrow Motors, LLC, was administratively

dissolved on February 4, 2020, by the North Carolina Secretary of State due to delinquency in filing the required 2019 annual report.

30. A LinkedIn account for Charisma Fozard listed her as affiliated with High Tide Legal. A web search for High Tide Legal in Durham, NC, revealed <https://hightide.law>. The website lists Charisma Fozard as the founding attorney at High Tide Legal. It describes Fozard as becoming a member of the South Carolina bar in 2018, and a member of the North Carolina bar in 2019. It further describes Fozard as being a paralegal for the North Carolina Department of Justice prior to becoming a solo practitioner. High Tide Legal is self-described as a law office established “to address the business and legal needs of entrepreneurs, small business owners, and non-profit organizations.” The High Tide Legal website lists the address as 2530 Meridian Parkway, Unit 2011, Durham, NC. No business registration was found on the North Carolina Secretary of State website for High Tide Legal. Surveillance of 2530 Meridian Parkway, Durham, NC, revealed that the second and third floor are operated by Regus. Regus provides business addresses with mail-handling service and virtual-office services. No signage at that location was observed for the Law Office of Charisma Fozard or High Tide Legal.

BIOMETRICS

31. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These

biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

32. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require.

33. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, if the device is equipped with an operating system that is earlier than version 9.3, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. If the operating system is version 9.3 or later, that time frame shrinks to 8 hours.

34. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints and thumbprints of any device's users to attempt to gain access to any Apple devices found pursuant to the search warrant. The government may not be able to obtain the contents of the Apple devices if those fingerprints are not used to access the Apple devices by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given Apple device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

35. In addition, I know from my training and experience that many other mobile device manufactures have their own version of Touch ID—that is, a fingerprint recognition feature that the device's user can program and use to unlock the device. For instance, I know that Google Pixel phones and Google Pixel XL phones have a fingerprint sensor that can be used to unlock the device. Similarly, Samsung, LG, HTC, and other manufacturers also have devices with fingerprint sensors.

36. Similarly, in my training and experience I know that some applications loaded onto mobile devices or other electronic devices may be secured by the user with a thumbprint or fingerprint. Common among these types of applications are applications such as mobile banking

apps or other financial applications, password storage applications, and secure communications apps, among others.

37. Further, if a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

38. Similarly, if a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-

sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

39. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

40. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

41. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose biometric features will unlock the device, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with

certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the Premises, Mazda 6, and GMC Yukon Denali to display one or more of the physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device covered by this search warrant, including to (1) press or swipe fingers (including thumbs) to the fingerprint scanner of the device(s); (2) hold the device(s) in front of a person's face to activate the facial recognition feature; and/or (3) hold the device(s) in front of a person's face to activate the iris recognition feature, for the purpose of unlocking the device(s) in order to search the contents as authorized by this warrant.

TECHNICAL TERMS

42. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service

providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

43. As described above and in Attachment B, this application seeks permission to search for records, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. *Probable cause.* I submit that if a computer or storage medium is found pursuant to the applied-for warrant, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

45. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium found pursuant to the applied-for warrant because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers,

e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs

may indicate whether the computer was remotely accessed, thus inculpatng or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant

insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

46. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu

of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge

that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data found pursuant to the applied-for warrant. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

48. I submit that this affidavit supports probable cause for a warrant to search the items described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

/s/ Kirk Ellis
Special Agent
Defense Criminal Investigative Service

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 2 day of November, 2020, at 3:12 a.m./p.m.


The Hon. Joi Elizabeth Peake
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 395 Shakespeare Drive, Morrisville, NC (hereinafter, "Premises"). The Premises comprises a two story townhouse as well as a detached garage in the rear of the property. The Premises is one of four townhouses connected together. The Premises is the second residence from the east side of the building. The front of the residence appears to be grey siding with blue shutters and a blue door. The house number, "395", appears on the right-most post of the front porch.

ATTACHMENT B

Property to be seized

1. All records and information relating to violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1030(a)(2) (Computer Fraud), 18 U.S.C § 1956 (Laundering of Monetary Instruments), and 18 U.S.C. § 1028A (Aggravated Identity Theft), those violations involving Marcus Thomas or Charisma Fozard and occurring after August 27, 2018, as follows:
 - a. Records and information relating to a conspiracy to defraud users of the Department of Defense's MyPay system;
 - b. Records and information relating to access of the Department of Defense's MyPay system;
 - c. Records and information relating to bank or other financial accounts, or financial transactions;
 - d. Debit/credit cards, debit/credit card statements, and debit/credit card applications in names other than Marcus Thomas and Charisma Fozard.
 - e. Records and information reflecting the purchase and/or deposit of money orders, pre-paid debit/credit cards, and gift cards;
 - f. Records and information reflecting the purchase, sale, and/or export of automobiles;

- g. Records and information, in names other than Marcus Thomas and Charisma Fozard, containing personally identifiable information such as social security numbers and dates of birth;
 - h. Identification documents and copies or representations thereof in names other than Marcus Thomas and Charisma Fozard, including driver's licenses, passports, military IDs, and school IDs;
 - i. Records and information relating to packages sent or received by postal methods, including the U.S. Postal Service, FedEx, and UPS;
 - j. Records and information relating to the receipt, transfer, or other disposition of any criminal proceeds, including bank statements; and
 - k. Currency in excess of \$1,000.00, prepaid credit cards, financial instruments (including stocks and bonds), crypto-wallets, and/or any other thing of value evidencing proceeds of financial crimes.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

- h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect COMPUTERS to the Internet.
5. During the execution of the search, law enforcement personnel are authorized to (1) press and/or swipe the fingers (including thumbs) of Marcus Thomas and/or Charisma Fozard to the fingerprint scanner of any COMPUTER found pursuant to the warrant and/or (2) hold any COMPUTER found pursuant to the warrant in front of the face of those same individuals to

activate the facial-recognition feature and/or iris-recognition feature of the COMPUTER, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant. This warrant does not authorize law enforcement personnel to compel other individuals found at the premises to provide biometric features, as described in this paragraph, to access or otherwise unlock any COMPUTER. Further, this warrant does not authorize law enforcement personnel to compel that Marcus Thomas and/or Charisma Fozard state or otherwise provide the password or any other means that may be used to unlock or access the COMPUTERS, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the COMPUTERS.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.